ARJIS TECHNICAL POLICY & PRIVACY OVERVIEW

February 3, 2016

ARJIS AUTOMATED REGIONAL JUSTICE INFORMATION SYSTEM

SANDAG

What is ARJIS?

- Joint Powers Agency (JPA) formed in 1981
- Division of San Diego Association of Governments
- 81 ARJIS local, state, and federal member agencies
- 47+ real-time interfaces
- Regional data accessible via a suite of applications
- Privacy and security protocols
- Secure access and auditing
- Technical policy development
  - Align with state and national policies

SANDAG

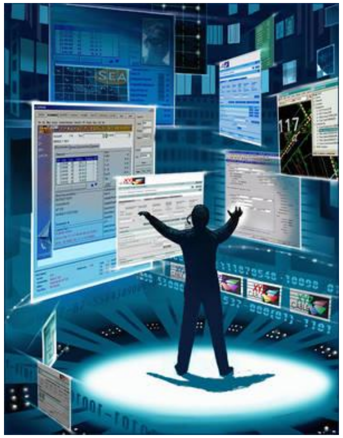
Overarching Policies

- California Department of Justice (CalDOJ)
- Master Control Agreement(MCA) between the San Diego County Sheriff’s Department (Sheriff) and ARJIS
- (FBI) Criminal Justice Information Services (CJIS) Security Policy (current rev. 8/4/2014)
- International Association of Chiefs of Police (IACP)
  - National policies and protocols
  - Developed the Model Technology Policy Framework

IACP TECHNOLOGY POLICY FRAMEWORK[1]
January 2014

Process for New Technologies

- Chiefs'/Sheriff's Management Committee recommends projects for annual work plan based on agency needs
- Develop and/or procure technology
- Complete Privacy Impact Assessment (PIA) and policy, approved by the SANDAG Public Safety Committee (PSC) and/or SANDAG Board
- Deploy technology
- Gather metrics, produce management reports
- Modify policy and PIAs as needed

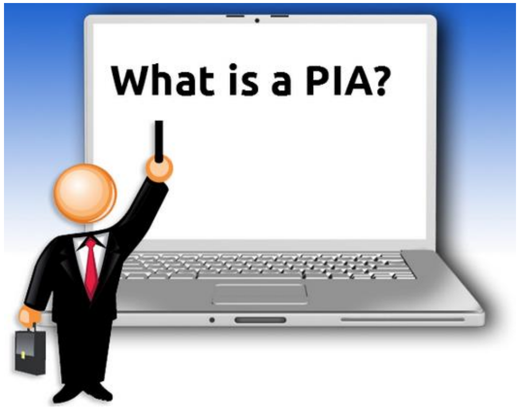


Privacy

Privacy Drivers- Laws Informing Integrated Justice Data

- The Privacy Act 1974 regulates how Federal agencies collect, maintain, use, and disclose an individual's information
  - Protects records about a person, such as education, financial, medical, criminal or work history
  - Requires records to be accurate, relevant, timely, and complete
  - Embodies Fair Information Practices Principles (FIPPS)
- E-Government Act 2002 requires Federal agencies to conduct PIAs

PIA Components



- What information is to be collected
- Why the information is being collected
- The intended use of the information
- With whom the information will be shared
- How the information will be secured
- Whether a system of records will be created

ARJIS PIAs

- ARJIS collaborates to ensure issues are addressed nationally:
  - White House Information Sharing Environment - ISE
  - Department of Homeland Security
  - FBI
- ARJIS partnered PIAs:
  - Booking data
  - Inter-state data sharing
    - Interstate sharing of photos
- Legislation
  - License Plate Reader(LPR)
    - Senate Bill 34 – Hill – October 2105
      - Privacy and Security Protections for Automated License Plate readers (LPR)

Privacy impact assessment report for the utilization of license plate readers

September 2009

International Association of Chiefs of Police
515 North Washington Street
Alexandria, Virginia, 22314

Policy

Process for ARJIS Policy Development

- Identify operational policy vs. technical policy components
- ARJIS responsible for the technical aspects of the regional technologies it maintains
  - Technical policy under the purview of the Public Safety Committee and SANDAG Board of Directors
- Individual agencies responsible for operational policies
  - Responsibility of the San Diego County Police Chiefs'/Sheriff's Association

ARJIS Technical Policy Topics

- Authorized access
- Audit services
- Physical and electronic security
- Data quality
- Retention
- System management and accountability
- Dissemination or release of data
- Performance Metrics

Authorized Access Only

- ARJIS public safety member agency;
  - Crtified with the California Department of Justice Law Enforcement Telecommunications System (CLETS);
  - Adheres to FBI-CJIS policies
  - All access is subject to audit
- ARJIS controls access by limiting users to only authorized law enforcement personnel
- Must enter 'reason' code

Audit capabilities

- All transactions are logged
- Logs are retained in accordance with retention policy
- Minimum audit information:
  - Name and ARJIS ID of the law enforcement user
  - Name of agency employing the user
  - Date and time of access
  - Reason for access

- Addressing misconduct is the responsibility of the agency
- ARJIS may limit or terminate system access in order to prevent misuse

Physical & Electronic Security

- Data and servers are hosted within the ARJIS secure infrastructure
  - Located in a secured law enforcement facility with multiple layers of physical security and 24/7 security protections
  - Physical access is limited to authorized technical staff

Data Quality

- ARJIS manages 111+ data validation tables to ensure data quality
- Data interfaces are monitored daily for accuracy and timely submission of data
- Alerts notify staff of incomplete data transfers
- Standardized the region’s FBI mandated crime reporting

Retention of Data

- ARJIS data conforms with state laws and/or statutes
- Lacking existing statutes, retention approved by the PSC and/or the SANDAG Board of Directors
- Based on review of existing retention polices of other agencies
- All interfaces must contain add, modify, and delete functionality for data integrity

System Management/Accountability

- ARJIS authorized technical staff manage the systems
- ARJIS meets both the CAL-DOJ CLETS and FBI CJIS Security Policies which include:
  - Government security compliance
  - Antivirus, firewalls
  - Encrypted communications
  - Measures to mitigate unauthorized access
- Provides 7/24 Help Desk support
- Responsible for system upgrades, back-ups, disaster recovery

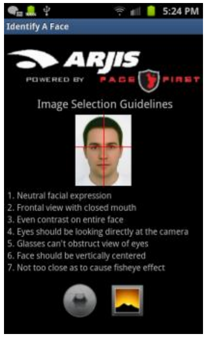


Image Selection Guidelines

1. Neutral facial expression
2. Frontal view with closed mouth
3. Even contrast on entire face
4. Eyes should be looking directly at the camera
5. Glasses can't obstruct view of eyes
6. Face should be vertically centered
7. Not too close as to cause fisheye effect

Dissemination or Release of Data

- ARJIS data is for official law enforcement purposes only
- Certain data is not subject to public disclosure as provided by 6254(f) of the California Government Code
- Data may also be exempt from disclosure under Section 6255 which provides for withholding of records when doing so is in the best interest of the public
- No personally identifying information shall be disseminated to members of the general public or news media

Performance Metrics

- Monthly management reports include:
  - Number of queries
  - Comparison to previous month and year
  - Effectiveness of the applications
  - Success stories
  - Any issues
- Annually and as needed monitor and evaluate the performance

Policies and PIAs – www.arjis.org

- ARJIS Joint Powers Agreement (JPA)
- ARJIS Acceptable Use Policy for Regional License Plate Readers
- License Plate Reader Privacy Impact Assessment
- ARJIS Acceptable Use Policy for Facial Recognition
- Facial Recognition Privacy Impact Assessment
- Draft Regional Data Sharing MOU

PAMELA SCANLON
ARJIS DIRECTOR
PSCANLON@ARJIS.ORG

ARJIS AUTOMATED REGIONAL JUSTICE INFORMATION SYSTEM

SANDAG